MASTER OF SCIENCE
IN
COMPUTER SCIENCE

IMPLEMENTATION OF A HYPERTEXT TRANSFER PROTOCOL SERVER ON A HIGH ASSURANCE MULTI-LEVEL SECURE PLATFORM
Evelyn Louise Bersack-Civilian, United States Army
B.S., University of Arizona, 1986
Master of Science in Computer Science-December 2000
Advisor: Cynthia Irvine, Department of Computer Science
Second Reader: Geoffrey Xie, Department of Computer Science

In a client/server environment on a local area network (LAN), a server should provide various network applications including a hypertext transfer protocol (HTTP) server. HTTP is a client/server, request/response application protocol that is used on the World Wide Web (WWW). It provides the definition and means for transferring objects across internets. A server used in the context of a multi-level secure (MLS) LAN should be no exception. A MLS LAN should be capable of providing an HTTP web server that can be used by commercially available web browsers executing on client workstations. This server needs to be aware of the MLS environment and provide clients access to all web pages and objects for which they are authorized.

This thesis implements an HTTP web server running on a high assurance host in a MLS LAN. The web server is based on a commercially available web server application. The commercially available application has been modified and configured to run on the high assurance host. This thesis discusses the details for implementing the web server on the high assurance host.

The result of this thesis is an HTTP web server application that runs on a high assurance host servicing clients on a MLS LAN that are using commercially available web browsers. These clients now have the capability of web browsing at varying levels of classification on one workstation.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Hypertext Transfer Protocol, Web Server, Multi-level Secure, Local Area Network, High Assurance

AN EXAMINATION OF POSSIBLE ATTACKS ON CISCO'S IPSEC-BASED VPN GATEWAYS
Joel R. MacRitchie-Lieutenant, United States Navy
B.S., United States Naval Academy, 1991
Master of Science in Computer Science-December 2000
Advisor: Daniel F. Warren, Department of Computer Science
Second Reader: John C. McEachen, II, Department of Electrical and Computer Engineering

Virtual Private Networks (VPNs) are an emerging security solution for computer networks in both the government and corporate arena. IPSec, the current standard for VPNs, offers a robust, standards-based, and cryptographically effective solution for VPN implementation. Because of the immense complexity of IPSec, effective analysis is difficult. In an environment where Information Warfare in general, and computer network attack in particular are becoming more pervasive, it is necessary conduct a critical, independent evaluation of IPSec from a security perspective.

In order to develop an effective evaluation of IPSec VPNs, a Cisco Systems IPSec-based VPN router network is used as an example. A detailed analysis of Cisco's IPSec-based implementation, as well as of the IPSec standard itself is conducted to determine what, if any, attacks or vulnerabilities exist in each.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Command, Control and Communications, Electronics, Electronic Warfare

KEYWORDS: Virtual Private Networks (VPN), Internet Protocol Security (IPSec), Computer Network Attack, Computer Security, Computing and Software, Network Security, Encapsulating Security Payload (ESP), Authentication Header (AH), Routers, Information Warfare (IW)

IMPLEMENTATION OF A TWO-USER DISPLAY USING STEREOSCOPICS
Susan C. Miller-Captain, United States Army
B.S., Northeast Louisiana University, 1988
Master of Science in Computer Science-December 2000
Advisor: Rudolph Darken, Department of Computer Science
Second Reader: Michael Capps, Department of Computer Science

The level of presence in a virtual environment depends on the extent to which the real world is shut out, the range of sensory elements the environment simulates, the extent of the panoramic view, and the resolution of the illusion. Many current virtual environment applications effectively address these presence issues for single users, but not for multiple users. Networked virtual environments address multiple user collaboration through real-time interaction of users in a shared environment. These systems provide effective communication between users, but do not address face-to-face collaboration.

To address these needs, this thesis describes a two-user display which fully supports face-to-face collaboration. Each user has independent views of the environment while standing near one another and is able to communicate through voice and gesture. The design of the system includes stereo rendering and magnetic tracking technology. Stereo rendering technology is used to create two separate images that can be viewed independently. A magnetic tracker is used to detect the movement of each user's head. There are drawbacks, including ghosting, that affect the design's usability. Studies are needed to determine appropriate application mediums for this type of system.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Human Systems Interface

KEYWORDS: Magnetic Tracking, Stereoscopy, Virtual Reality